

Integrate with Cisco Cyber Vision

- ISE pxGrid , on page 1
- ISE-API, on page 1
- XDR, on page 2
- Secure Remote Access, on page 5
- Cisco In Product Support, on page 9

ISE pxGrid

Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat-control platform that enables seamless integration among multivendor identity, network, security, and asset management systems.

You can configure Cisco ISE pxGrid integration from the **Platform Exchange Grid** page.

To access the **Platform Exchange Grid** page, choose **Admin** > **Integrations** > **ISE - pxGrid** from the main menu.

For more information about this integration, refer to the *Integrating Cisco Cyber Vision with Cisco Identity Services Engine (ISE)* manual.

ISE-API

Security Group Tags (SGTs) are 16-bit labels assigned to devices or groups of devices to define their roles and associated security policies within a network.

Using Cisco Cyber Vision, you can map static subnets, network-based groups, or user-defined groups directly to SGTs. A secure, active Cisco Identity Services Engine (ISE) API connection enables the automatic synchronization of these mappings from Cisco Cyber Vision to Cisco ISE. This integration allows you to effectively enforce TrustSec policies across your network.

To create IP-to-SGT mappings based on group definitions, choose **Admin** > **Integrations** > **ISE – API** from the main menu.

For further details on IP-to-SGT mapping, refer to the *Integrate Cisco Cyber Vision with Cisco Identity Services Engine (ISE)* manual.

XDR

The Cisco Cyber Vision XDR integration connects Cisco Cyber Vision with Cisco XDR, a cloud-native, built-in platform that connects the Cisco Secure portfolio with your infrastructure.

Cisco XDR centralizes security events from Cisco software through an API. It can receive and correlate Cisco Cyber Vision events and firewall activities, then present them in dashboards.

The integration can significantly reduce dwell time and human-powered tasks.

The XDR integration enables the following three features in Cisco Cyber Vision:

- Without XDR SSO login, **Investigate in XDR Threat Response** appears on component technical sheets.
- With XDR SSO login, **Report to XDR** appears for certain events on the event calendar page. Use **Report to XDR** to send these events to XDR.
- With XDR SSO login, you can activate the **XDR ribbon** in Cisco Cyber Vision to access its features.



Note SecureX reached end of life on 2024-07-31.

Configure XDR

Configure the XDR integration in Cisco Cyber Vision.

Before you begin

Before you begin, ensure that you have Admin access to Cisco Cyber Vision Center, a Cisco Cyber Vision Center with internet access, and an XDR account with an admin role.

Procedure

Step 1 From the main menu, choose **Admin** > **Integrations** > **XDR**.

Step 2 Click the **Region** drop-down list and select a region.

Step 3 Select **Enable XDR** to enable the link.

The control turns red to indicate **Disable XDR**.

You can now use **Investigate in XDR Threat Response**, which appears in the component technical sheet. Complete the remaining steps to install and use the XDR ribbon and **Report to XDR**.

Step 4 In the upper-right corner of the GUI, open the user menu and select **My Settings**.

An **XDR** menu appears on the right side of the **My Settings** page.

Step 5 Click **Log in**.

A **Grant Application Access** popup appears with an authentication code.

Step 6 Click **Verify and Authorize**. In the **Security Cloud Sign On** window that opens, enter **Email** and click **Continue** to grant Cisco Cyber Vision access to **XDR**.

Step 7 Click **Authorize Cyber Vision**.

A **Client Access Granted** popup appears. In **Cisco Cyber Vision Center** > **My Settings**, the **XDR** menu indicates that Cisco Cyber Vision is connected to XDR.

Step 8 Use the **Ribbon status** toggle to enable the XDR ribbon.

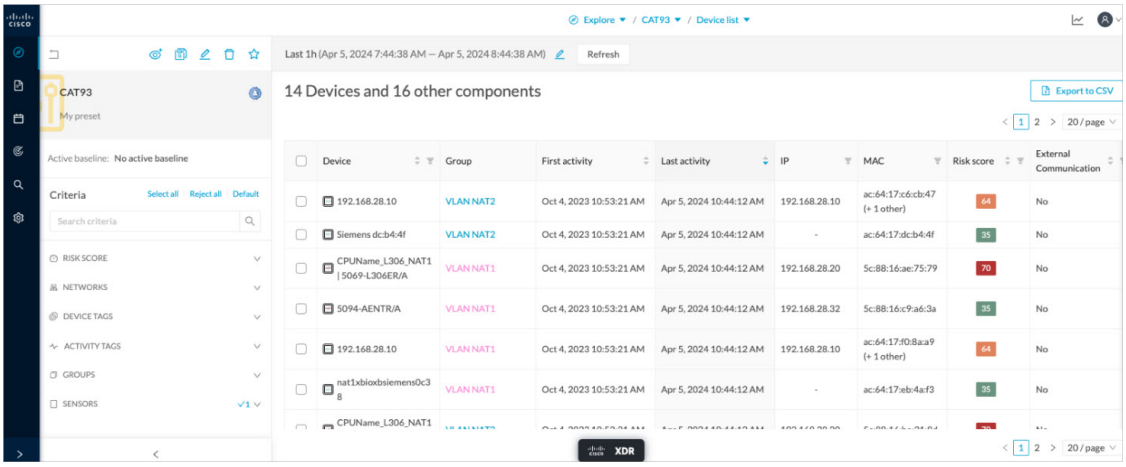
After you enable **Ribbon status**, a message appears.

Step 9 To log out, click **Logout of XDR**, then click **Save settings**.

XDR Ribbon

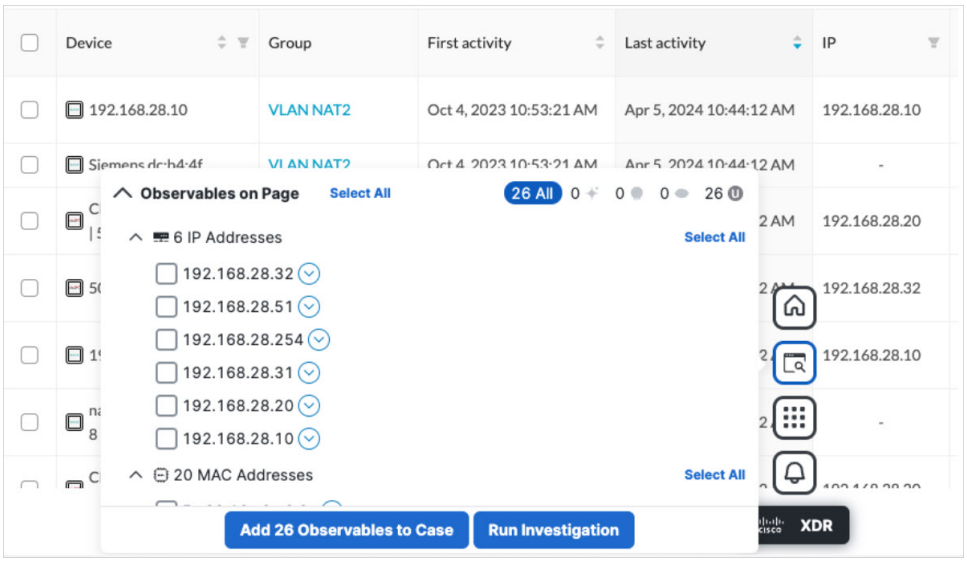
The XDR ribbon appears at the bottom of the Cisco Cyber Vision GUI in the Explore menu once it is configured and activated.

The XDR ribbon in the Device List view:



The Cisco XDR Getting Started Guide explains how to use the XDR ribbon.

For example, to find observables and investigate them in XDR Threat Response, click the **Find Observables** icon like below:



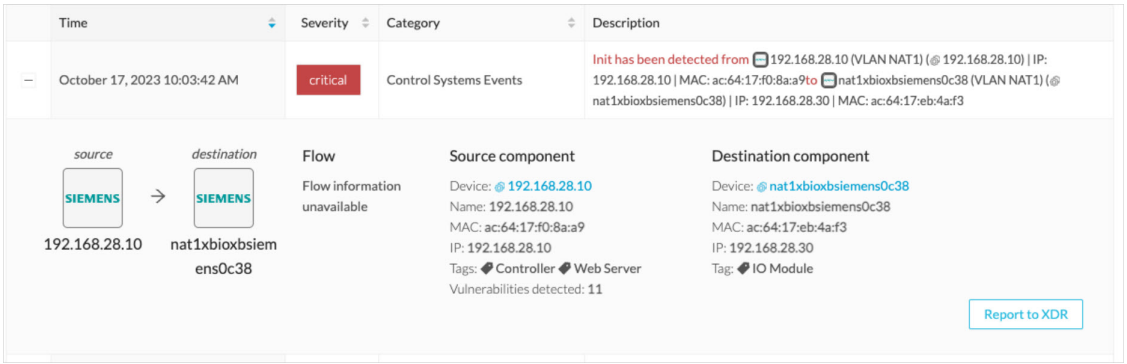
XDR Event Integration

After configuring XDR in Cisco Cyber Vision, the **Report to XDR** button appears for some events on the event calendar page. Selecting this button sends the event to XDR and creates an incident.

The **Report to XDR** button is available for the following event categories:

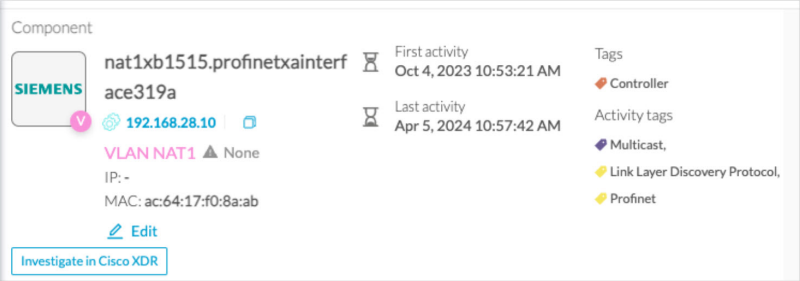
- Anomaly Detection
- Control Systems Events
- Signature Based Detection

Figure 1: Report to XDR button on a Control Systems Event



XDR component button

After you configure XDR in Cisco Cyber Vision, the **Investigate in Cisco Threat Response** button appears on the component's technical sheet. If you use this button, XDR Threat Response investigates the component's IP and MAC addresses.



External resources for XDR integration

Provides the necessary URLs for Cisco XDR integration across different geographic regions to facilitate secure communication.

Center:

North America

- Cisco XDR Platform: https://visibility.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.us.security.cisco.com/api/

Europe

- Cisco XDR Platform: https://visibility.eu.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.eu.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.eu.security.cisco.com/api/

Asia Pacific, Japan, and China

- Cisco XDR Platform: https://visibility.apjc.amp.cisco.com/iroh/
- Cisco XDR Private Intelligence: https://private.intel.apjc.amp.cisco.com/ctia/
- Cisco XDR Automation: https://automate.apjc.security.cisco.com/api/

Web client:

- conure.apjc.security.cisco.com
- conure.us.security.cisco.com
- conure.eu.security.cisco.com

Secure Remote Access

A secure equipment access solution is a Cisco offering that

- provides secure remote access for operations teams to manage and troubleshoot operational technology assets,

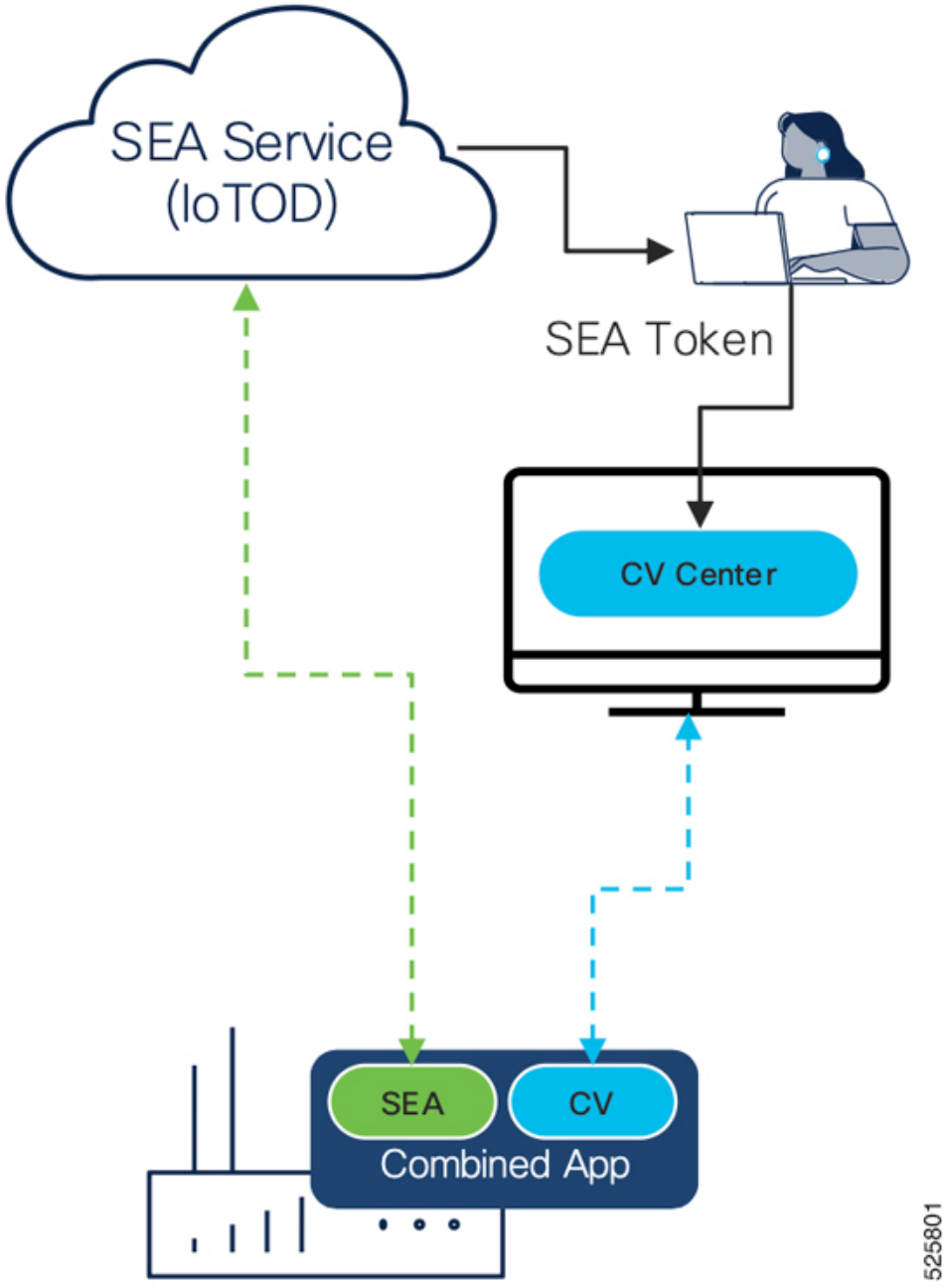
- eliminates the need for costly on-site service visits,
- enables Zero Trust Network Access gateway functionality.

For more details, see the SRA documentation.

Integration with Cyber Vision

You can integrate SRA with Cyber Vision for unified management in the Cyber Vision Center. The integration requires the SRA agent (an IOx application) to run on your network device. You install the SRA agent and the Cyber Vision sensor app with the same workflow. One IOx application packages both runtimes.

Figure 2: Integrate Cyber Vision with SRA



Feature history table

Feature	Release Information	Feature Description
Enable Cyber Vision Center as an SRA Gateway	Release 5.5.x	The Secure Remote Access agent can run directly on the Cyber Vision Center. This setup eliminates the need to host the agent within an IOx application. When you enable the Center as an SRA gateway, you provide secure, remote access to the Center and its network resources through the IoT Operations Dashboard. You do not need direct inbound access.

Integrate Cisco Cyber Vision Center with SRA

Enable SRAmless, unified management of Secure Equipment Access (SRA) and Cisco Cyber Vision through Cisco Cyber Vision Center. The integration simplifies deployment and ongoing management of both components on the same device while keeping their operations separate.

Before you begin

Ensure that you have administrative access to Cisco Cyber Vision Center and tenant administrator access to the SRA organization that you intend to connect with Cisco Cyber Vision.

Procedure

Step 1 Log in to Cisco Cyber Vision Center, and then choose **Admin** > **Integrations** > **SRA** from the main menu.

Step 2 On the **SRA** page, in the **Configuration** section, select a region from the drop-down list and click **Connect**.

Step 3 Log in to the **IoT Operations Dashboard** with your IoT OD credentials.

Step 4 On the **IoT Operations Dashboard**, click **Connect**.

Step 5 On the **SRA** page, verify the details in the **Configuration** section.

Step 6 Click **Enable SRA**.

Step 7 (Optional) Click **Validate configuration** to validate the configuration.

A success message appears on the **SRA** page, indicating that SRA is configured.

What to do next

Install the compatible sensors. For more information, refer to the “Install sensors with the sensor management extension” topic in the *Cisco Cyber Vision Sensor Application for Cisco Switches Installation Guide*.

Enable Cyber Vision Center as an SRA Gateway

Configure your Cyber Vision Center as a Secure Equipment Access (SRA) gateway.

Enabling Cyber Vision Center as an SRA gateway removes the need for an external IOx application. This setup offers secure remote support and allows centralized asset management through the IoT Operations Dashboard.

Before you begin

Ensure your Cyber Vision Center is connected to SRA.

Procedure

Step 1 Log in to Cyber Vision Center.

Step 2 From the main menu, choose **Admin** > **Integrations** > **SRA**.

Step 3 (Optional) In the **Center as gateway** section, optionally enter a name for your center.

If you do not add a center name, Cyber Vision Center uses the Center's Fully Qualified Domain Name (FQDN) from **Admin** > **Web Server Certificate**.

Step 4 Click **Enable Center as Gateway**.

- Your Cyber Vision Center contacts the SRA tenant and registers itself as a new SRA agent. Log in to SRA and choose **System Management** > **Network Devices** to view the new agent. The new network device appears in the list.
- Once you enable Center as gateway, a direct link to the IoT OD SRA dashboard becomes available. If you have access to multiple tenants in IoT OD, select the correct tenant to view your new network device.

What to do next

Add new assets to your center as needed. These assets will be reachable through your Center, which now acts as a gateway. You can manage and access other assets directly from the Center. For more information, see Manually Add Assets in the IoT Operations Dashboard (IoT OD) documentation.

Cisco In Product Support

A **Cisco In Product Support** is a virtual assistant that:

- provides customers and partners with a unified self-service experience across multiple support domains,
- offers tools for managing cases, checking bug applicability, troubleshooting hardware, and managing licensing, and
- enables users to connect directly with case owners, managers, or Technical Assistance Center (TAC) duty managers for escalations or assistance.

Feature History

Table 1: Feature History Table

Feature	Release information	Feature description
Cisco In Product Support	Release 5.3.x	Use **Cisco In Product Support** to manage your Cisco support cases and related tasks directly from the Center.

Support capabilities

Cisco In Product Support is designed to simplify and speed up support activities for Cisco customers and partners.

By using a single interface that consolidates multiple support services, you can address technical challenges and manage support team interactions efficiently.

The tool integrates with Cisco's back-end systems to provide up-to-date case tracking, bug search, and device troubleshooting resources.

Support activity examples

- A partner uses **Cisco In Product Support** to submit and track a hardware replacement (RMA) request.
- A customer uses **Cisco In Product Support** to check whether a reported bug affects their installed software version.
- A network engineer uses the self-service troubleshooting function to diagnose hardware issues without opening a formal support ticket.

Access Cisco In Product Support

Open **Cisco In Product Support** to interact with Cisco TAC support from your product.

Cisco In Product Support provides integrated access to Cisco TAC services. You can use **Cisco In Product Support** to open TAC cases, record screens, or upload files directly from your product interface.

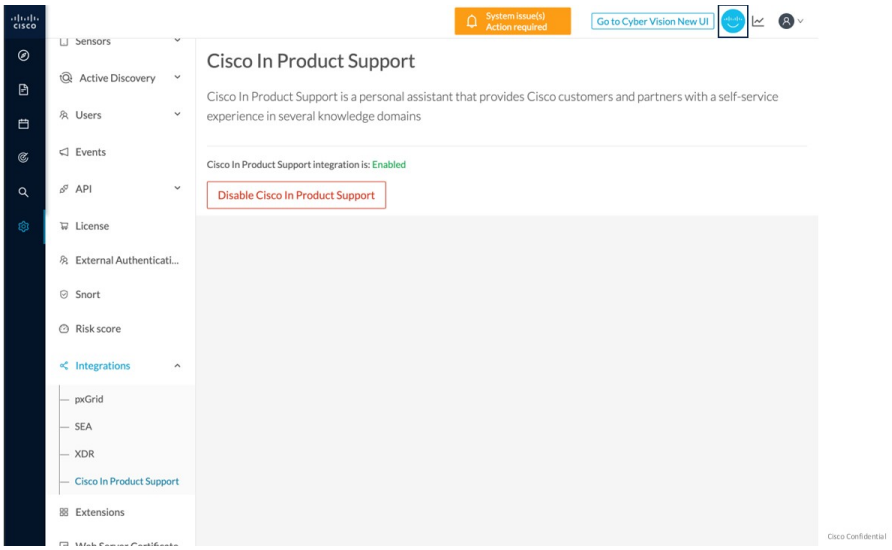
Note The **Cisco In Product Support** integration is enabled by default, and its icon is available on the page.

Before you begin

Ensure that you have a Cisco account with TAC access.

Procedure

Step 1 From the main menu, choose **Admin** > **Integrations** > **Cisco In Product Support**.



Step 2 Click **Cisco In Product Support**.

Step 3 Click **Sign In** to enable TAC virtual assistance.

After you enable Cisco In Product Support, you can:

- Open support cases with **Open Cisco Support Case**.
- Record your screen with **Record Screen**.
- Upload files with **Upload Local File**.

What to do next

To generate and upload diagnostics, select **System Statistics**.